REMARKS/ARGUMENTS

Prior to this amendment, claims 1-33 were pending with claims 16-33 being withdrawn. In this amendment, claims 1, 10, and 15 are amended. Claims 16-33 are canceled. Claims 34-51 are added. Thus, after entry of this amendment, claims 1-15 and 34-51 will be pending.

Interview

Applicants would like to thank the Examiner for extending the courtesy of a telephone interview with counsel, David B. Raczkowski, on November 19, 2007.

Rejections under 35 USC 102(e), Graham

Claims 1-15 are rejected under 35 USC 102(e) as being anticipated by *Graham et al.* (US 7,237,264 B1).

Claims 1-14, 34-39

Claim 1 is allowable as Graham does not teach or suggest each and every element of claim 1. For example, claim 1 recites:

> *(a) detecting an occurrence of a security event within a customer network, wherein detecting includes ascertaining at least one parameter associated with the security event and determining an importance of the security event based on the parameter;*
> *(b) querying a first component of the customer network for data in response to the detected occurrence of the security event;*
> *(c) receiving, by a data monitor located within the customer network, first data from the component in response to the query;*
> *(d) determining, based on the received first data, whether to query for additional data;*
> *(e) querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step.*

Graham describes a system for preventing network misuse. *See Graham*, abstract. A node 132 may detect an incident directed to another node 134 in the LAN 140. *Id.*, col. 4 lines 45-48. Based on a variety of factors, an alert condition or precautionary measures may be taken by node 132. *Id.*, col. 4 lines 48-58. The precautionary measures include blocking incoming data. *Id.*, col. 7 lines 65-67. Note that listening for a target's response is not an active

step of querying and receiving a response to the query. *Id.*, col. 8 lines 5-9. The only mention of a query is a scanner making a query as to what services/applications are running on a target. *Id.*, col. 6 lines 60-66.

Thus, although many factors may be used to determine a response to the security event, the result of a first query is not used to determine whether another query should be made. Graham does not mention additional queries, let alone new queries based on a response to a first query. Accordingly, Graham does not teach or suggest "*determining, based on the received first data, whether to query for additional data*" and "*querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step*," as recited in claim 1.

Furthermore, the determination of the data signature of the security event cannot correspond to "*querying a first component of the customer network for data in response to the detected occurrence of the security event.*" The determination of the data signature and the context in which the data signature is transmitted occur at a detection stage, and do not occur in response to the detected security event. *Id.*, col. 5 lines 59-67. Thus, the only query presented to a component on the LAN 140 and suggested by Graham remains the one by the scanner. *Id.*, col. 6 lines 60-66. Accordingly, although Graham may use a table containing a target fingerprint and a data signature, Graham does not mention a second query based on the first query. *Id.*, FIG. 6 and col. 7 lines 14-57.

For at least these reasons, claim 1 is allowable over Graham. As claim 1 is allowable, dependent claims 2-14 and 34-39 are also allowable for at least the same rationale.

Claim 9

In addition to being allowable for the same rationale as claim 1, claim 9 is allowable for additional reasons. For example, claim 9 recites "*transmitting the received first data to a security analysis module for analysis.*" At page 5, the Office Action states that claims 8-10 and 13-14 recite the same limitations as claims 1-7. However, claim 9 recites a "security analysis module." Claims 1-7 do not recite this claim element, thus the Office Action has not stated where the above limitation is found in Graham. Applicants submit that Graham does not

mention a security analysis module and a data monitor that receives the first data. For at least this additional reason, claim 9 is allowable over the cited references.

Claim 15

Applicants submit that claim 15 should be allowable for at least the same rationale as discussed with respect to claim 1.

Claims 40-51

Claim 40 is allowable as Graham does not teach or suggest each and every element of claim 40. For example, claim 40 recites:

> *analyzing the security event using at least one of the first data and the additional data, wherein analyzing the security event is performed by a security analysis module that is not part of the customer network.*

In Graham, one or more nodes of a LAN 140 perform monitoring and analysis. *Id.*, col. 4 lines 45-48 and col. 12 lines 33-43. Graham does not mention a device outside of the LAN 140 performing any monitoring or analysis. In fact, Graham specifically displays other networks, but does not describe any interaction between network 140 and the devices of the other networks regarding the prevention of misuse of network 140. *Id.*, FIG. 2. Thus, Graham teaches away from such an interaction. Accordingly, Graham does not teach or suggest the above limitation.

For at least these reasons, claim 40 is allowable over Graham. As claim 40 is allowable, dependent claims 41-51 are also allowable for at least the same rationale.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

/David B. Raczkowski/

David B. Raczkowski
Reg. No. 52,145

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
DBR:scz
61182805 v1